UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,486	11/19/2003	Masahiro Fukui	60188-697	4493

7590 09/22/2006

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
GEBRESILASSIE, KIBROM K	

ART UNIT	PAPER NUMBER
2128	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/715,486	FUKUI ET AL.	
	Examiner	Art Unit	
	Kibrom K. Gebresilassie	2128	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 10/715,486.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/03 and 03/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the application filed on November 19, 2003.

2. Claims 1-17 are examined.

Priority

3. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119 (a-d) or 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on November 19, 2003 and March 16, 2004 are considered.

Oath/Declaration

5. The Office acknowledges receipt of properly signed oath/declaration filed November 19, 2003.

Claim Objections

6. Applicant is advised that should claim 1 be found allowable, claim 9 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,076,060 issued to Bilchev et al, in view of US Publication No. 2002/0083330 issued to Shiomi et al.

As per Claim 1:

Bilchev discloses an apparatus comprising:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1);

storage means for storing encrypted circuit information (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230);

stored circuit information decrypting means for reading out the encrypted circuit information from the storage means, decrypting the circuit information (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61), and

providing the decrypted circuit information (analogous to "The deciphered data block can then be output to the output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43);

intermediate data encrypting means for encrypting intermediate data generated during a simulation and storing the encrypted intermediate data in the storage means (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means, decrypting the intermediate data (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40), and

providing the decrypted intermediate data (analogous to "The deciphered data block can then be output to the output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 2:

Bilchev discloses the circuit operation simulating apparatus of claim 1, wherein the stored circuit information decrypting means and the intermediate data decrypting means are combined together (analogous to "Because the cipher units are reversible,

the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61).

As per Claim 3:

Shiomi discloses the circuit operation simulating apparatus of claim 1, including intermediate data deleting means for deleting the intermediate data stored in the storage means, after the simulation has been terminated (analogous to "..removal of an overlapping dummy circuit..." [0051]).

As per Claim 4:

Bilchev discloses an apparatus comprising: circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1);

supplied circuit information decrypting means for decrypting supplied circuit information encrypted by a first encryption technique (Fig. 3 element 40a);

stored circuit information encrypting means for encrypting, by a second encryption technique (Fig. 3 element 40b), the circuit information decrypted by the supplied circuit information decrypting means (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage

of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

storage means for storing the circuit information encrypted by the second encryption technique (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230); and

stored circuit information decrypting means for reading out the circuit information encrypted by the second encryption technique from the storage means, decrypting the circuit information, and providing the decrypted circuit information (analogous to "The deciphered data block can then be output to the output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "...conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi

related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 5:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the encryption by the first encryption technique has an encryption strength higher than that by the second encryption technique (col. 12 lines 54-58).

As per Claim 6:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the encryption by the second encryption technique requires shorter time for encryption and decryption than that by the first encryption technique (analogous to "..the cipher unit 40a to 40d are coupled sequentially." Col. 5 lines 57-61).

As per Claim 7:

Bilchev discloses the circuit operation simulating apparatus of claim 4, wherein the circuit information decrypted by the supplied circuit information decrypting means is not stored in the storage means but encrypted by the stored circuit information encrypting means (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3

lines 51-54; Fig. 10 element 230).

As per Claim 8:

Bilchev discloses the circuit operation simulating apparatus of claim 4, including:

intermediate data encrypting means for encrypting intermediate data and for storing the encrypted intermediate data in the storage means (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means , decrypting the intermediate data, and providing the decrypted intermediate data (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40),

wherein the stored circuit information encrypting means and the intermediate data encrypting means are combined together (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 9:

Bilchev discloses a circuit operation simulating apparatus comprising:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1); and

storage means for storing encrypted circuit information (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is

instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230),

wherein the circuit operation simulating apparatus is configured to be able to incorporate: stored circuit information decrypting means for decrypting the encrypted circuit information read out from the storage means (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61) and

intermediate data encrypting means for encrypting intermediate data generated during a simulation by the simulation means and for storing the encrypted intermediate data in the storage means (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29); and

intermediate data decrypting means for decrypting the encrypted intermediate data read out from the storage means (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40) and

for providing the decrypted intermediate data (analogous to "The deciphered data block can then be output to the output device which can then either output each of the

data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 10:

Bilchev discloses a circuit operation simulating apparatus comprising:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1); and

storage means for storing encrypted circuit information, wherein the circuit operation simulating apparatus is configured to be able to incorporate (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230):

supplied circuit information decrypting means for decrypting supplied circuit information encrypted by a first encryption technique (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61; Fig. 3 element 40a);

stored circuit information encrypting means for encrypting, by a second encryption technique (Fig. 3 element 40b),

the circuit information decrypted by the supplied circuit information decrypting means, and for storing the encrypted circuit information in the storage means; and

stored circuit information decrypting means for decrypting the circuit information read out from the storage means and encrypted (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher

units to be used but in reverse order for deciphering." Col. 3 lines 56-61) by the second encryption technique (Fig. 3 element 40b), and

for providing the decrypted circuit information (analogous to "The deciphered data block can then be output to the output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 11:

Bilchev discloses a circuit operation simulating method comprising:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1);

a stored circuit information decrypting step of reading out encrypted circuit information from storage means and decrypting the circuit information for use in the simulation step (analogous to "The deciphered data block can then be output to the output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43);

an intermediate data encrypting step of encrypting intermediate data generated during a simulation in the simulation step and of storing the encrypted intermediate data in the storage means (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29); and

an intermediate data decrypting step of reading out the encrypted intermediate data from the storage means and decrypting the intermediate data (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 12:

Bilchev discloses a method comprising:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1);

a supplied circuit information decrypting step of decrypting supplied circuit information encrypted by a first encryption technique (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted

by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

a stored circuit information encrypting step of encrypting, by a second encryption technique (Fig. 3 element 40b), the circuit information decrypted in the supplied circuit information decrypting step (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61) and of storing the encrypted circuit information in storage means (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230); and

a stored circuit information decrypting step of reading out the circuit information encrypted by the second encryption technique from the storage means and of decrypting the circuit information for use in the simulation step (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 13:

Bilchev discloses program which makes a computer execute:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1);

a stored circuit information decrypting step of reading out encrypted circuit information from storage means and decrypting the circuit information for use in the simulation step (analogous to "The deciphered data block can then be output to the

output device which can then either output each of the data blocks sequentially or wait until the complete signal has been deciphered before outputting it." Col. 8 lines 39-43);

an intermediate data encrypting step of encrypting intermediate data generated and of storing the encrypted intermediate data in the storage means (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29); and

an intermediate data decrypting step of reading out the encrypted intermediate data from the storage means and decrypting the intermediate data (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for

doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 14:

Bilchev discloses a circuit operation simulating program which makes a computer execute:

circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1); and

a supplied circuit information decrypting step of decrypting supplied circuit information encrypted by a first encryption technique (Fig. 3 element 40a), a stored circuit information encrypting step of encrypting, by a second encryption technique (Fig. 3 element 40b), the circuit information decrypted in the supplied circuit information decrypting step and of storing the encrypted circuit information in storage means (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61), and

a stored circuit information decrypting step of reading out the circuit information encrypted by the second encryption technique from the storage means and of decrypting the circuit information for use in the simulation step (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 15:

Bilchev discloses supplied circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1), the system comprising:

encryption means for encrypting circuit information to be supplied (Fig. 11 element 300);

transmission means for transmitting the encrypted circuit information via a network reception means for receiving the transmitted circuit information (analogous to "A modem is provided for connection over a telecommunications line to transmit and receive enciphered data. Also a network card is provided for connection over a network to transmit and receive data." Col. 9 lines 13-16; Fig. 14);

storage means for storing the received circuit information (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230);

stored circuit information decrypting means for reading out the encrypted circuit information from the storage means and decrypting the circuit information (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is

possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

receiving the decrypted circuit information from the stored circuit information decrypting means (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

intermediate data encrypting means for encrypting intermediate data generated and storing the encrypted intermediate data in the storage means (analogous to "Enciphered data is received by the enciphered data input device and is formed into enciphered data blocks by the enciphered data block former. The passage of enciphered data blocks into a working memory..." col. 8 lines 26-29); and

intermediate data decrypting means for reading out the encrypted intermediate data from the storage means, decrypting the intermediate data, and providing the decrypted intermediate data (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual

output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 16:

Bilchev discloses supplied circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1), the system comprising:

first encryption means for encrypting circuit information to be supplied, by a first encryption technique (Fig. 3 element 40a);

transmission means for transmitting the encrypted circuit information via a network, reception means for receiving the transmitted circuit information (analogous to "A modem is provided for connection over a telecommunications line to transmit and

receive enciphered data. Also a network card is provided for connection over a network to transmit and receive data." Col. 9 lines 13-16; Fig. 14);

first decrypting means for decrypting the received circuit information (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

second encryption means for encrypting, by a second encryption technique (Fig. 3 element 40b), the circuit information decrypted by the first decrypting means (Fig. 4 element 40d); storage means for storing the circuit information encrypted by the second encryption technique (analogous to "The invention is equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230);

second decrypting means for reading out the circuit information encrypted by the second encryption technique from the storage means and for decrypting the circuit information (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61); and

receiving the decrypted circuit information from the second decrypting means (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

As per Claim 17:

Bilchev discloses supplied circuit information on a configuration and characteristics of the circuit (analogous to "....which generates the circuits and simulates them or using electronic hardwired circuits. ...with storage medium storing

logic to configure the PLGA to carry..." col. 11 lines 48-54; Fig. 1), the system comprising:

first encryption means for encrypting circuit information to be supplied, by a first encryption technique (Fig. 3 element 40a);

second encryption means for further encrypting, by a second encrypted technique, the circuit information encrypted by the first encryption technique (Fig. 3 element 40b);

transmission means for transmitting the circuit information encrypted by the second encryption technique, via a network ; reception means for receiving the transmitted circuit information (analogous to "A modem is provided for connection over a telecommunications line to transmit and receive enciphered data. Also a network card is provided for connection over a network to transmit and receive data." Col. 9 lines 13-16; Fig. 14);

first decrypting means for decrypting the received circuit information encrypted by the second encryption technique and for outputting the circuit information encrypted by the first encryption technique (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61);

storage means for storing the circuit information output from the first decrypting means and encrypted by the first encryption technique (analogous to "The invention is

equally applicable to the encryption of a signal which is not transmitted and which is instead stored securely e.g. the encryption and storage of data in a computer to prevent unauthorised access." Col. 3 lines 51-54; Fig. 10 element 230);

second decrypting means for reading out the circuit information encrypted by the first encryption technique from the storage means and for decrypting the circuit information (analogous to "Because the cipher units are reversible, the encipher apparatus and decipher apparatus can be constituted by a single apparatus. Thus, the duplex communication of an encrypted signal or for storage of encrypted data for retrieval and decryption it is possible for the same cipher units to be used but in reverse order for deciphering." Col. 3 lines 56-61); and

receiving the decrypted circuit information from the second decrypting means (analogous to "Once all of the cipher units defined by the circuit array have been implemented in reverse and thus the enciphered data block has been deciphered,...The deciphered data block can then be output to the output device...." Col. 8 lines 35-40).

Bilchev fails to disclose simulation means for simulating operation of a circuit.

Shiomi discloses simulation means for simulating operation of a circuit (analogous to "..conducting a simulation for actual design data to obtain an actual output value, conducting simulation for the reference operation model to obtain an expected output value." [0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Bilchev related to a cipher in which the secret cipher code which is required for both enciphering and deciphering is information

which describes the process used to carry out enciphering with the teachings of Shiomi related to a technology for maintaining confidentiality of design data. The motivation for doing so would have been more convenient to verify encrypted circuit design data by simulation, wherein verifying steps limits the simulation conducted by unauthorized access [0012]. Hence a skilled artisan having access to the teaching of Bilchev and Shiomi would have knowingly modified the teaching of Bilchev with Shiomi.

Conclusion

1. Claims 1-17 are rejected.

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Scott Hauck, Stephen Knol, "Data Security for Web-based CAD", IEEE 1998, pgs 1-16.

3. Any inquiring concerning this communication or earlier communication from the examiner should be directed to Kibrom K. Gebresilassie whose telephone number is (571) 272-8571. The examiner can normally be reached on Monday-Friday, 8:30 am to 4:30 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner supervisor, Kamini shah can be reached at (571) 272-2279. The official fax number is (571) 273-8300. Any inquiring of a general nature relating to the status of this application should be directed to the group receptionist whose telephone number is (571) 272-3700.

Kibrom K. Gebresilassie
Patent Examiner
U.S. Patent and Trademark Office

Simulation and Emulation, Art Unit 2128
401 Dulany St., Room 5C25 (Randolph)
Alexandria, VA 22314-5774
Tel: 571-272-8571
Kibrom.gebresilassie@uspto.gov

Thai Phan
Patent Examiner
AU 2128